ЛАБОРАТОРНАЯ РАБОТА

НАСТРОЙКА СЕТЕВОЙ ПОДСИСТЕМЫ ЗАЩИЩЕННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

Задание на лабораторную работу

1. Настроить стенд в соответствии с приведенными требованиями к стенду. Сервер должен иметь статические сетевые адреса, заканчивающиеся на единицу, сохраняющиеся после перезагрузки компьютера. Клиенты должны получать IP-адрес автоматически по протоколу DHCP.

2. На сервере настроить DHCP-сервер. Диапазон выдаваемых IP-адресов в каждом сегменте должен быть 101 – 200.

3. На сервере настроить DNS-сервер, имя домена стенда – «localdomain», настроить прямую зону – для домена и две обратные зоны – по одной для каждой подсети.

4. Настроить автоматическую регистрацию выданных DHCP-сервером IP-адресов в сервере DNS.

5. Продемонстрировать работоспособность стенда после перезагрузки всех компьютеров:

- продемонстрировать отсутствие информации в файлах hosts;
- продемонстрировать работоспособность сервера DHCP (работающий сервис, выдача IP-адресов, регистрация адресов в DNS-сервере);
- продемонстрировать работоспособность сервера DNS (работающий сервис, результаты команд PING, DIG, NSLOOKUP для всех сетевых имен компьютеров стенда, а также виртуальных имен).

УКАЗАТЕЛЬ

Требования к стенду

Модель автоматизированной системы, с которой будут проводится практические занятия и лабораторная работа, представляет собой совокупность виртуальных машин, объединенных в сеть, одна из виртуальных машин играет роль сервера, две остальные – рабочей станции. На сервере установлена ОС Linux (Debian, Ubuntu), на рабочих станциях Linux (Debian, Ubuntu) и Windows XP или выше. Схема стенда приведена на Рисунок 0.1. На рисунке, кроме того приведены адреса подсетей сетевых адаптеров виртуальных машин, где XX – вариант выполнения задания (порядковый номер студента в списке группы).

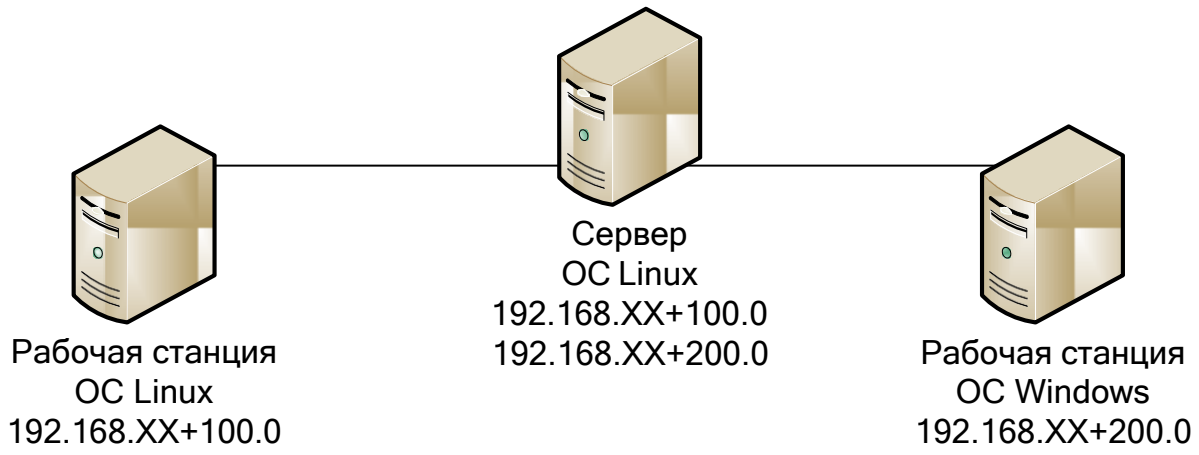

Рисунок 0.1 – Схема стенда

Кроме того, необходимо произвести следующие настройки виртуальных машин:

- размер оперативной памяти – 2048 Мбайт;
- количество процессоров – 1;
- количество ядер процессора – 1;
- объем жесткого диска – 10 Гбайт.

Сервер должен иметь два сетевых адаптера, один из которых соединен напрямую с сетевым адаптером рабочей станции под управлением ОС Linux, второй – с сетевым адаптером рабочей станции под управлением ОС Windows. Сервер должен иметь сетевые адреса, заканчивающиеся на единицу, рабочие станции должны получать сетевой адрес по DHCP.

Сетевые имена виртуальных машин (XX – вариант выполнения задания):

- сервера – servXX;
- рабочей станции Linux – linXX;
- рабочей станции Windows – winXX.

Краткие теоретические сведения

DHCP (Dynamic Host Configuration Protocol) – протокол динамической настройки узла, позволяющий автоматически получать IP-адреса и настройки сети.

Позволяет автоматизировать процесс настройки параметров сети, когда все настройки определяются на сервере DHCP и выдаются клиентам по запросу. Такая централизация позволяет, во-первых, упростить процесс настройки сети в едином месте, во-вторых, не допустить конфликтов, в случае конфликтующих настроек клиентов. Все изменения необходимо вносить только на сервере DHCP, настройки будут получены клиентами автоматически, что удобно при динамически меняющемся составе сети. Кроме IP-адреса и маски подсети могут выдаваться параметры адресов шлюзов, контроллеров домена, сервера DNS, имени домена и т.п.

DNS (Domain Name System) – служба имен домена позволяет производить преобразование символьного имени компьютера в его IP-адрес и обратно. Использование имен компьютеров является более удобным для человека, чем запоминать IP-адреса компьютеров, особенно при их большом количестве и динамически меняющемся составе сети. При работе совместно с DHCP сервер DNS позволяет автоматически регистрировать у себя соответствие имени компьютера и выданного автоматически IP-адреса.

Доменная структура DNS представляет собой древовидную иерархию, состоящую из узлов, зон, доменов, поддоменов и др. элементов. «Вершиной» доменной структуры является корневая зона. Настройки корневой зоны расположены на множестве серверов/зеркал, размещенных по всему миру и содержат информацию обо всех серверах корневой зоны, а также отвечающих за домены первого уровня (ru, net, org и др). Зоной в терминологии DNS является любая часть дерева системы доменных имен, размещаемая как единое целое на неко-

тором DNS-сервере, являющаяся зоной ответственности этого сервера. Зоны делятся на прямые и обратные. Прямая зона хранит информацию и позволяет преобразовать сетевое имя в сетевой адрес. Обратная зона позволяет преобразовать сетевой адрес в сетевое имя. Для одной и той же сети количество прямых и обратных зон может отличаться, количество прямых зон определяется количеством доменов и поддоменов сети, а количество обратных зон определяется количеством подсетей. На примере нашей работы – имеется единый домен, назовем его «locadomain», поэтому прямая зона будет одна, а количество подсетей – две: 192.168.XX+100 и 192.168.XX+200, поэтому обратных зон будет две.

В рамках данной работы, стенд представляет собой единый домен, и задачей сервера DNS является только разрешение сетевых имен в сетевые адреса, задачи построения и настройки многоуровневых доменов в данной работе не решаются.

Использование данных сервисов позволяет существенно упростить процесс администрирования вычислительной сети и снять нагрузку с администраторов.

Методические рекомендации

Вся приведенная информация в методических рекомендациях относится к варианту 0, то есть имя сервера будет serv00. Кроме того, расписываются варианты настройки только одного сегмента 192.168.100.0.

При наличии готовой виртуальной машины проводить установку пакетов нет необходимости.

Начальная настройка стенда

При необходимости получения прав суперпользователя на продолжительный период использовать команду

```
sudo su -
```

Для однократного получения прав суперпользователя при исполнении некоторой команды:

```
sudo команда
```

До начала установки серверов необходимо сконфигурировать стенд, а именно объединить компьютеры в сеть, настроить сетевые адреса сервера и имена всех компьютеров. Сетевые адреса рабочих станций должны получаться по DHCP.

Для установки сетевого имени в ОС Linux необходимо воспользоваться утилитой **hostnamectl**:

```
hostnamectl set-hostname HOSTNAME
```

Информация об имени хранится в файле /etc/hostname, но его напрямую нежелательно.

Проверить текущее имя можно выполнив команду **hostnamectl** без параметров или **hostname**.

Для установки сетевого имени в ОС Windows 7 необходимо вызвать «Свойства системы», далее нажать кнопку «Изменить» (См. Рисунок 0.2). Здесь же можно проверить текущее имя. Интерфейс в других версиях ОС Windows не сильно отличается и имеет схожий порядок действий для изменения или проверки сетевого имени.

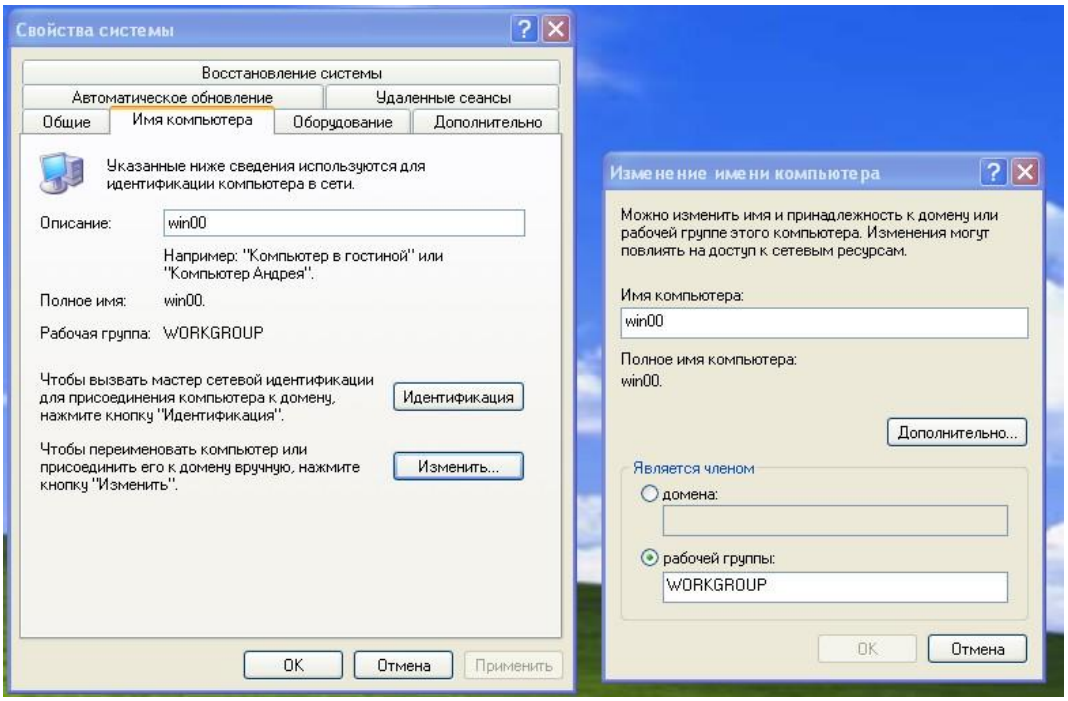

Рисунок 0.2 – Изменение сетевого имени в ОС Windows XP

Для установки сетевого адреса сервера с ОС Linux необходимо модифицировать конфигурационный файл /etc/network/interfaces. Для каждого сетевого соединения в файле /etc/network/interfaces необходимо прописать необходимые настройки, например:

```
auto enp0s9
    iface enp0s9 inet static
    address 192.168.100.1
```

```
netmask 255.255.255.0
```

После установки сетевых адресов необходим убедиться, что заданные адреса назначаются интерфейсам после перезагрузки сервера.

Установка сервера DHCP

Установка сервера DHCP производится на компьютере стенда, выполняющего роль сервера.

В данном разделе приведена информация о настройке сервера DHCP, работающего в независимости от наличия сервера DNS. Все необходимые дополнительные настройки сервера DHCP для работы с сервером DNS приведены в разделе по установке и настройке сервера DNS.

Проверить наличие пакетов сервера DHCP и при необходимости установить.

Проверка выполняется командой:

dpkg –s isc-dhcp-server

При необходимости установки пакета ввести команду:

apt install isc-dhcp-server

Необходимо настроить сетевые интерфейсы, на которых будет работать сервер DHCP, для этого в файле /etc/default/isc-dhcp-server изменить параметр INTERFACES (имена интерфейсов могут отличаться):

```
INTERFACES=”ens33 ens34”
```

Для каждой подсети, в которой будет работать сервер DHCP, необходимо произвести настройки в файле **/etc/dhcp/dhcpd.conf** – создать два раздела для каждо- го сегмента сети (ZZ – номер подсети):

```
subnet 192.168.ZZ.0 netmask 255.255.255.0{
option routers 192.168.ZZ.1;
option subnet-mask 255.255.255.0;
option domain-name-servers 192.168.ZZ.1;
range dynamic-bootp 192.168.ZZ.101 192.168.ZZ.200;
default-lease-time 600;
max-lease-time 7200;   }
```

Добавить в начала файла директиву, указывающую, что данный DHCP-сервер является главным сервером в сегменте.

```
authoritative;
```

Дополнительную информацию по настройке конфигурационного файла dhcpd.conf, при необходимости, можно получить выполнив команду:

man dhcpd.conf

Далее для проверки работоспособности запустить сервер DHCP в ручном режиме командой

dhcpd

Успешный результат, показывающий, что сервер работает на двух сетевых интерфейсах приведен ниже, указано, что сервер принимает запросы на определенных сетевых интерфейсах, в случае неуспеха будет выведена та или иная ошибка с описанием. После проверки необходимо убить процесс сервера (kill -9 <номер процесса dhcpd>).

```
Internet Systems Consortium DHCP Server 4.3.2
Copyright 2004-2015 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Not searching LDAP since ldap-server, ldap-port and ldap-
base-dn were not specified in the config file
Config file: /etc/dhcpd.conf
Database file: /var/lib/dhcpd/dhcpd.leases
PID file: /run/dhcpd/dhcpd.pid
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 1 leases to leases file.
Listening on LPF/ens37/00:0c:29:ab:7a:ca/
192.168.200.0/24
Sending on   LPF/ens37/00:0c:29:ab:7a:ca/
192.168.200.0/24
Listening on LPF/ens33/00:0c:29:ab:7a:c0/
192.168.100.0/24
```

```
Sending on   LPF/ens33/00:0c:29:ab:7a:c0/
192.168.100.0/24
Sending on   Socket/fallback/fallback-net
```

Далее необходимо настроить автоматический запуск сервера при загрузке компьютера.

Включить сервис для автоматической загрузки:

systemctl enable dhcpd

Запустить DHCP сервер:

systemctl start dhcpd

Проверить текущее состояние:

systemctl status dhcpd

Дополнительную информацию по ключам команды systemctl можно посмотреть в конце данного раздела или получить, выполнив команду:

man systemctl

В случае возникновения ошибок при запуске сервера DHCP, подробный отчет об ошибках и сообщения сервера можно посмотреть командой

journalctl –xe –u dhcpd

Необходимо добиться состояния, когда сервис dhcpd запускается автоматически после запуска компьютера.

Установка сервера DNS

Роль сервера DNS выполняет сервер Berkley Internet Name Domain (BIND).

Необходимо проверить наличие пакетов сервера и при необходимости установить.

Проверить их наличие можно командой:

dpkg –s bind9

При необходимости установки пакетов выполнить команду:

apt install bind9

За работу сервера DNS отвечает служба named.

Проверить, что все пакеты успешно установлены:

named -v

Для возможности обновления информации в DNS необходимо использовать ключ, разрешающий проводить обновление информации только доверенным серверам или клиентам. В нашем случае информацию будет обновлять сервер DHCP, сообщая серверу DNS какому клиенту, какой IP-адрес был выдан.

Можно использовать существующий по умолчанию ключ, который расположен в файле /etc/bind/rndc.key. В файле указано, что существует ключ с именем **rndc-key**, который сгенерирован по алгоритму HMAC-MD5. Сам ключ приведен после параметра secret (может отличаться).

```
$ cat /etc/bind/rndc.key
key rndc-key {
    algorithm hmac-md5;
    secret
"xcrzoluCn8HkluQBEKggoJPQUYPt7mDjvBd0nLNwtBLB7Aeqlgo29piZIln
x";
};
```

Данный ключ используется, в том числе, при работе данного DNS-сервера с вышестоящими DNS-серверами, поэтому при работе в многоуровневой сети с несколькими DNS-серверами для решения задачи обновления информации от DHCP-сервера рекомендуется использовать отдельный ключ. **В рамках данной работы, генерировать отдельный ключ не обязательно.**

Будем минимально модифицировать установленный по умолчанию DNS сервер, в частности, не будем настраивать отдельный домен, а будем модифицировать информацию о домене localdomain.

Информация о зонах находится в файле настроек /etc/bind/named.conf.

Если, как раньше определялось, для обновления информации от DHCP сервера используется ключ по умолчанию, то информацию о нем в файл конфигурации вносим (если данной строки нет) строкой:

```
include "/etc/bind/rndc.key";
```

Далее остальные настройки будут указываться для ключа по умолчанию **rndc-key**.

Нам необходимо будет редактировать файл /etc/bind/named.conf.local.

Необходимо найти в данном файле найти информацию о зоне localdomain и внести в нее указание об используемом для обновления информации ключе.

```
zone "localdomain" IN {
        type master;
        file "master/localdomain.zone";
        allow-update { key rndc-key; };
};
```

Параметр **type** содержит информацию о типе DNS-сервера, значение **master** означает первичный DNS-сервер, **slave** – вторичный. Параметр **file** указывает, в каком файле находится информация о настройках зоны, (путь к файлу указывается относительно каталога /etc/bind/, то есть в данном случае полное имя /etc/bind/master/localdomain.zone). Параметр **allow-update** содержит информацию о разрешении обновления инфомрации зо- ны, здесь указывается либо ключ, либо значение **none;**

Далее необходимо создать разделы с информацией об обратных зонах, (будет приведен пример для **одной** зоны 192.168.100.). Для обратных зон используются служебные домены in-addr.arpa (IPv4) и ip6.arpa (IPv6):

```
zone "100.168.192.in-addr.arpa" IN {
        type master;
        file "reverse/named.100";
        allow-update { key rndc-key;};
    };
```

Проведем настройку прямой зоны localdomain в файле /etc/bind/master/localdomain.zone. Поскольку мы работаем с одним доменом, то **можно оставить приведенные значения параметров по умолчанию**. В противном случае необходимо заменить @ (которая означает имя текущего домена) на полное имя домена, localhost на полное имя сервера, например «serv00.localdomain», root на короткое имя сервера «serv00».

В конце файла **необходимо** указать дополнительную информацию об узлах сети, имеющих статические адреса(в том числе сам сервер), или несколько се-

тевых имен для одного сетевого адреса **(это потребуется в дальнейших работах).** Например, запись вида

```
serv00           IN  A     192.168.100.1
serv00-virtual       IN  CNAME    serv00
serv00-virtual2  IN  CNAME    serv00
```

означает, что сервер с именем serv00 имеет сетевой адрес 192.168.101.1, а serv00-virtual и serv00-virtual2 это виртуальные сетевые имена, перенаправляемые на serv00.

Особенность прямой зоны – указывается одно соответствие IP-адреса имени, то есть если ваш сервер имеет больше одного IP-адреса необходимо указывать разрешение имени только в один IP-адрес.

Настройку обратных зон на примере зоны 192.168.100. проведем в файле /etc/bind/reverse/named.100. В итоге должен получиться файл следующего содержания (измененные параметры подчеркнуты, обратите внимание на наличие пробела между кратким именем serv00 и полным именем сервера serv00.localdomain во второй строке файла настроек):

```
$TTL 86400
@       IN SOA serv00.  serv00.localdomain.  (
                        1997022700 ; Serial
                        28800      ; Refresh
                        14400      ; Retry
                        3600000    ; Expire
                        86400 )    ; Minimum
100.168.192.in-addr.arpa. IN NS serv00.
1.100.168.192.in-addr.arpa. IN PTR serv00.
1.100.168.192.in-addr.arpa. IN PTR serv00-virtual.
1.100.168.192.in-addr.arpa. IN PTR serv00-virtual2.
```

Запись в конце файла с параметром NS (Name Server) указывает на сервер DNS, параметр PTR (pointer) отображает IP-адрес в доменное имя.

Файлы обратных зон допускают полное и краткое написание адреса компьютера, например, последние строки указанной выше конфигурации могут быть записаны как:

```
              IN  NS serv00.
1             IN PTR serv00.
1             IN PTR serv00-virtual.
1             IN PTR serv00-virtual2.
```

То есть имя обратной зоны при кратком написании не указывается, а указывается только адрес. Обратите внимание что, для указания записи о сервере имен (NS) **вообще не указывается никакого адреса,** поскольку запись NS определяет

адрес или имя сервера DNS для текущей зоны.

Сопряжение серверов DHCP и DNS

В настройках DHCP-сервера необходимо добавить параметры обновления записей DNS-сервера, для этого в файле /etc/dhcp/dhcpd.conf изменить значение параметра ddns-update-style на interim, а также добавить несколько параметров в общую часть, в части, касающиеся настройки подсетей, также необходимо будет добавить информацию о ключе обновления и зонах.

В итоге файл конфигурации для **одной подсети** будет выглядеть следующим образом (возможны отличия по вариантам, значению ключа и т.п., вновь появившиеся и измененные параметры выделены):

```
ddns-update-style interim;
update-static-leases on;
ddns-updates on;
ddns-domainname "localdomain";
authoritative;
subnet 192.168.100.0 netmask 255.255.255.0 {
    option routers 192.168.100.1;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.100.1;
    range dynamic-bootp 192.168.100.50 192.168.100.99;
    default-lease-time 600;
    max-lease-time 7200;
    ddns-rev-domainname "in-addr.arpa.";
    option domain-name "localdomain";
}
key rndc-key {
    algorithm hmac-md5;
    secret
"xcrzoluCn8HkluQBEKggoJPQUYPt7mDjvBd0nLNwtBLB7Aeqlgo29piZ
Ilnx";
```

```
};
zone localdomain. {
     primary 127.0.0.1;
     key rndc-key;
     }
zone 100.168.192.in-addr.arpa. {
     primary 127.0.0.1;
     key rndc-key;
     }
```

После внесения изменений в настройках DHCP-сервера необходимо его перезапустить командой:

```
systemctl restart dhcpd
```

Далее необходимо настроить автоматический запуск DNS-сервера при загрузке системы командами:

```
systemctl enable bind9
systemctl start bind9
```

Добавить в файл /etc/resolv.conf информацию о поиске имен компьютеров по умолчанию в домене localdomain, файл должен содержать следующую информацию (в зависимости от варианта):

```
nameserver 192.168.100.1
search localdomain
domain localdomain
```

Проверка сервера DHCP

Проверка со стороны клиента. Для проверки работы сервера DHCP необходимо настроить сторону клиента на автоматическое получение сетевого адреса

по протоколу DHCP, после чего перезапустить сетевую службу клиента или перезапустить ОС клиента полностью.

После этого необходимо убедиться в получении сетевых настроек – для этого любым известным образом проверить сетевой адрес клиента (например, команды ifconfig для ОС Linux, ipconfig для ОС Windows).

Проверка со стороны сервера. Для проверки выдачи сетевого адреса клиенту необходимо проверить файлы аудита для службы dhcpd с использованием любой из команд

```
journalctl -xe -u dhcpd
cat /var/log/messages | grep dhcpd
cat /var/log/syslog | grep dhcpd
```

Результат будет содержать информацию о выдаче конкретного сетевого адреса конкретному клиенту, кроме того, при настройке обновления информации в DNS информация об этом будет также отображаться (См. Рисунок 0.3)

Для проверки корректной работы сервера DHCP и сервера DNS, необходимо проверить добавление информации в DNS сервер о выделенных сервером DHCP сетевых адресах. Это отображается, во-первых, в файлах аудита системы, как приведено на рисунке, а также записывается в файлы прямых и обратных зон, расположенных в каталогах /etc/bind/master и /etc/bind/reverse, которые мы настраивали ранее.

```
dhcpd[36458]: DHCPDISCOVER from 00:0c:29:d3:ef:28 via ens37
dhcpd[36458]: DHCPOFFER on 192.168.201.2 to 00:0c:29:d3:ef:28
              (win00) via ens37
dhcpd[36458]: DHCPREQUEST for 192.168.201.2 (192.168.201.1)
              from 00:0c:29:d3:ef:28 (win00) via ens37
dhcpd[36458]: DHCPACK on 192.168.201.2 to 00:0c:29:d3:ef:28
              (win00) via ens37
dhcpd[36458]: Added new forward map from win00.localdomain
              to 192.168.201.2
dhcpd[36458]: Added reverse map from
              2.201.168.192.201.168.192.in-addr.arpa to
              win00.localdomain
```

Рисунок 0.3 – Пример информации о выделении IP-адреса и обновлении информации в DNS сервере

Для форсирования обновления IP-адреса клиента необходимо выполнить команды:

В ОС Windows:

```
ipconfig /release
ipconfig /renew
```

В ОС Linux:

```
dhclient –v –r ens33
ifconfig ens33 down
ifconfig ens33 up
```

В качестве ens33 необходимо указать корректное название сетевого интерфейса, либо вообще не указывать сетевой интерфейс.

Первая команда освобождает занятый адрес, вторая запрашивает новый адрес (В случае с ОС Linux вместо второй команды используется выключение и включение сетевого интерфейса, что приводит к перезапросу сетевого адреса, поскольку в данной версии ОС команда dhclient не посылает серверу DHCP корректное сетевое имя, что приводит к отсутствию обновления DNS записей).

Проверка сервера DNS

Проверку можно производить как со стороны сервера, так и со стороны клиента, указанные далее утилиты установлены по умолчанию в пакете bind-utils.

Необходимо запросить разрешение имен в IP-адреса для всех трех компьютеров стенда как по коротким именам, например, serv00, так и по полным, например, serv00.localdomain.

Команда **HOST** – утилита для обращения к системе DNS.

```
host serv00.localdomain
```

Результат выполнения команды выдает хранящееся на сервере DNS соответствие имен и IP-адресов, при их отсутствии – информацию об ошибке (Рисунок 0.4). Команде можно передавать как сетевое имя компьютера, так и его IP-адрес (См. Рисунок 0.6).

```
serv00 reverse # host win00
win00.localdomain has address 192.168.100.128
serv00 reverse # host win00.localdomain
win00.localdomain has address 192.168.100.128
serv00 reverse # host win10.localdomain
Host win10.localdomain not found: 3(NXDOMAIN)
```

Рисунок 0.4 – Пример ответа команды host

Команда **NSLOOKUP** – утилита для обращения к системе DNS.

Команде можно передавать либо сетевой адрес (См. Рисунок 0.6), либо сетевое имя (См. Рисунок 0.5), при этом в зависимости от настроек сервера возможны отличия при передаче полного сетевого имени (win00.localdomain) и неполного сетевого имени (win00).

```
Serv00 ~ # nslookup win00
;; Got SERVFAIL reply from 192.168.101.1, trying next server
Server:         192.168.201.1
Address:        192.168.201.1#53

** server can't find win00: SERVFAIL

Serv00 ~ # nslookup win00.localdomain
Server:         192.168.101.1
Address:        192.168.101.1#53

Name:   win00.localdomain
Address: 192.168.201.2

Serv00 ~ # nslookup 192.168.201.2
** server can't find 2.201.168.192.in-addr.arpa: NXDOMAIN

Serv00 ~ # nslookup 192.168.201.1
1.201.168.192.in-addr.arpa      name = Serv00.
```

Рисунок 0.5 – Пример работы команды NSLOOKUP

Пример запроса на получение сетевого имени по IP-адресу приведен на рисунке (См. Рисунок 0.6)

```
serv00 reverse # host 192.168.100.128
128.100.168.192.in-addr.arpa domain name pointer win00.localdomain.
serv00 reverse # nslookup 192.168.100.128
128.100.168.192.in-addr.arpa    name = win00.localdomain.
```

Рисунок 0.6 – Пример получения информации по IP-адресу

Команда **DIG** – утилита для обращения к системе DNS.

```
dig serv00.localdomain
```

```
; <<>> DiG 9.11.4-P1 <<>> serv00
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Рисунок 0.7 – Пример ответа о некорректно работающем сервере

```
; <<>> DiG 9.11.0-P2 <<>> Serv00.localdomain
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 64167
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7ce8b9f863ca3c1722fda1345be5ba060a6e89bff144e9bb (good)
;; QUESTION SECTION:
;Serv00.localdomain.            IN      A

;; AUTHORITY SECTION:
localdomain.           86400   IN      SOA     localhost.localdomain.
                                               root.localdomain. 43
;; Query time: 0 msec
;; SERVER: 192.168.101.1#53(192.168.101.1)
;; WHEN: Fri Nov 09 19:47:02 MSK 2018
;; MSG SIZE  rcvd: 126
```

Рисунок 0.8 – Пример ответа о корректно работающем сервере

Выполнив указанную команду, где serv00 – имя сервера, можно получить ответ, свидетельствующий либо об отсутствии или некорректной работе сервера (См. Рисунок 0.7), либо о корректной его работе (См. Рисунок 0.8)

После того, как некоторый клиент получил по DHCP сетевой адрес и настройки сети, то со стороны сервера можно также попытаться проверить информацию о клиенте командой dig и получить ответ (См. Рисунок 0.9).

`dig win00.localdomain`

```
; <<>> DiG 9.11.0-P2 <<>> win00.localdomain
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2411
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 976df925c1c89aa2133946c85be5b9efb3b0b8f0317cdbd8 (good)
;; QUESTION SECTION:
;win00.localdomain.             IN      A

;; ANSWER SECTION:
win00.localdomain.      300     IN      A       192.168.201.2

;; AUTHORITY SECTION:
localdomain.           86400   IN      NS      localhost.localdomain.

;; ADDITIONAL SECTION:
localhost.localdomain.  86400   IN      A       127.0.0.1

;; Query time: 0 msec
;; SERVER: 192.168.101.1#53(192.168.101.1)
;; WHEN: Fri Nov 09 19:46:39 MSK 2018
;; MSG SIZE  rcvd: 130
```

Рисунок 0.9 – Пример ответа о клиенте

Команда **PING**

При передаче в качестве аргумента команде сетевого имени узла должно произойти преобразование сетевого имени в сетевой адрес с использованием DNS-сервера. При работающем сервере DNS результат будет успешным (См.

Рисунок 0.10), в противном случае – нет (См. Рисунок 0.11).

```
PING win00.localdomain (192.168.201.2) 56(84) bytes of data.
64 bytes from 192.168.201.2: icmp_req=1 ttl=128 time=0.771 ms
64 bytes from 192.168.201.2: icmp_req=2 ttl=128 time=0.436 ms
64 bytes from 192.168.201.2: icmp_req=3 ttl=128 time=0.395 ms
```

Рисунок 0.10 – Пример при работающем DNS сервере

```
ping: unknown host win00
```

Рисунок 0.11 – Пример при неработающем DNS сервере

Настройка клиента DNS

Основная необходимость взаимодействия клиента и сервера DNS это потребность клиента, работающего в сети, устанавливать четкое соответствие между сетевыми адресами и сетевыми именами компьютеров. Решить эту задачу можно различными способами.

Первый способ – указание четкого соответствия между сетевыми адресами и сетевыми именами на стороне клиента. Производится это в файле /etc/hosts.

Второй способ – использование DNS.

Существуют также другие способы, связанные с использованием протоколов WINS, NETBIOS или баз данных, но их мы рассматривать не будем.

Для повышения достоверности результата все эти способы используются одновременно, но с указанием приоритета, то есть если не было найдено локального соответствия в файле /etc/hosts, то необходимо обратиться к DNS серверу и так далее. Приоритет или порядок обращения настраивается в параметре hosts файла **/etc/nsswitch.conf.** По умолчанию, установлен следующий приоритет – сначала локальный файл /etc/hosts, далее DNS-сервер.

```
hosts: files dns
```

Другие параметры можно изучить, выполнив команду

```
man nsswitch.conf
```

Для настройки клиента DNS необходимо в сетевых настройках указать сетевой адрес сервера DNS.

Если клиент получает настройки автоматически через DHCP, то информацию о сервере DNS необходимо внести в состав настроек, получаемых автома-

тически, как это описывалось ранее.

Возможные проблемы и типовые ошибки

1) При установке пакетов **dhcpd** или **bind9** могут возникнуть проблемы отсутствия тех или иных зависимых пакетов. Информация об этом будет выведена при попытке установить пакеты.

2) При запуске служб **dhcpd** или **bind9** в случае их неправильной настройки будут выведена информация о невозможности запуска службы и информация по ошибке.

Более подробную информацию можно получить в файлах аудита системы, выполнив команды (одну на выбор):

```
systemctl status имя_службы
journalctl –xe –u имя_службы
cat /var/log/messages
cat /var/log/syslog
```

Далее в зависимости от вида ошибки необходимо устранить ее причину.

3) Если ошибка запуска DHCP связана с отсутствием или невозможностью записи в файл **/var/lib/dhcp/dhcpd.leases**, то:

при необходимости создать указанный каталог и файл

```
mkdir /var/lib/dhcp
touch /var/lib/dhcp/dhcpd.leases
```

проверить и при необходимости установить владельца файлов и каталога на **isc-dhcpd**

```
chown isc-dhcpd.isc-dhcpd /var/lib/dhcp
chown isc-dhcpd.isc-dhcpd /var/lib/dhcp/dhcpd.leases
chown isc-dhcpd.isc-dhcpd /var/lib/dhcp/dhcpd.leases~
```

(при наличии)

проверить и при необходимости установить права 755 на каталог /var/lib/dhcp

chmod 755 /var/lib/dhcp

проверить и при необходимости установить права 644 на файл /var/lib/dhcp/dhcpd.leases

chmod 644 /var/lib/dhcp/dhcpd.leases

4) Если при запуске сервиса DHCP выдается ошибка о достижении предельного количества запусков **start-limit-hit**, то необходимо выполнить следующую команду, после чего запустить сервис снова.

systemctl reset-failed dhcpd

5) Если запрос к DNS-серверу работает по полному имени (serv00.localdomain), но не работает по короткому (serv00), необходимо проверить файл /etc/resolv.conf, в нем должно быть три строчки:

```
nameserver 192.168.100.1
search localdomain
domain localdomain
```

Для того, чтобы внесенные изменения в файл /etc/resolv.conf не были отменены службой NetworkManager необходимо в файле /etc/NetworkManager/NetworkManager.conf в разделе [main] добавить параметр

```
dns=none
```

Формат команд

systemctl – команда управления сервисами

без ключей – показывает все запущенные службы;

--failed – показывает все незапущенные из-за ошибки;

start XX – запустить службу XX;

stop – остановить службу XX;

status XX – проверить статус службы XX, будет выведен текущий статус и сообщения об ошибках (аналог сокращенного journalctl);

restart XX – перезапуск службы XX;

enable XX – включить службу XX (автозагрузка при включении системы);

disable XX – выключить службу XX из автозагрузки;

is-enabled XX – проверить автозагрузку службы XX;

reboot – перезапустить систему;

poweroff – выключить систему;

hibernate – перевести систему в режим гибернации.

journalctl – команда просмотра журнала событий

без ключей – все события;

-b – с момента загрузки ОС;

-b -1 – предыдущая загрузка ОС;

-b -2 – предпредыдущая загрузка ОС;

-k – просмотр сообщений ядра;

-n 20 – последние 20 сообщений;

-e – перейти в конец журнала;

-x – показывать расшифровки сообщений;

-f – в реальном масштабе времени;

-u – фильтрация по имени службы;

fullpath/*name* - вывод событий конкретного приложения;

_PID/_UID/_GUID=XX - вывод по PID, UID, GUID;

-p XX – фильтрация по уровню ошибки (0 до 7);

0 — EMERG (система неработоспособна).

7 —DEBUG (отладочные сообщения).

hostnamectl – команда изменения сетевого имени

без параметров – просмотреть текущее имя

set-hostname NAME – установить имя NAME

Кроме того необходимо проверить файл hosts в котором указано соответствие имени и адреса 127.0.0.1